UTKARSH MATHUR

+1 (919)-349-6756 | u7karsh@yahoo.co.in | www.u7karsh.com | u7karsh | utkarshmathur

RESEARCH INTERESTS

Computer architecture with special interests in high-performance microarchitecture, General Purpose Computation on Graphics Processors (GPGPU), and architectural support for security.

EDUCATION

NC State University — *Raleigh, NC*

*M.S. Electrical and Computer Engineering (**GPA:** 4.238/4)* — *August, 2017 - May, 2019*

- **Courses Taken:** Microprocessor Architecture, Architecture of Parallel Computers, ASIC Design with Verilog, Advanced Microarchitecture, Advanced Architecture on Data Parallel Processors, Operating Systems Design, Cryptographic Engineering and Hardware Security

COMPUTER/SOFTWARE SKILLS

Languages C/C++, CUDA, Verilog, SystemVerilog, Python, Assembly for RISC-V, Java, PHP, SQL, CQL

Packages GPGPU-sim, 721sim (cycle-accurate RISC-V superscalar simulator), MATLAB, ModelSim, Synopsys Design Vision, LaTeX

WORK EXPERIENCE

Marvell Semiconductors — *Santa Clara, CA*

Architecture Engineer — *August, 2019 - Present*

- Part of the ThunderX4 server processor architecture team working on multiple pipeline stages

Cadence Design Systems — *Noida, India*

R&D Engineer — *July, 2015 - July, 2017*

- Development in Verification IP for the protocols HDMI, MHL & I2c
- Co-created a component-based methodology with the aim to have more scalable and flexible architecture of Verification IPs and reduced time to market
- Created features like Consumer Electronics Control (CEC) Physical Layer, adDDC from scratch
- Co-created TripleCheck solution for USB Type C

M.S. THESIS & RESEARCH

NC State University — *Raleigh, NC*

Research Assistant — *May, 2018 - May, 2019*

- Post Silicon Micro-architecture implementation of CLEAR (Checkpointed Load EArly Retirement) under Prof. Eric Rotenberg which is a high performance microarchitecture for CPUs as a part of my M.S. Thesis
- Architectural support for mitigating timing based side channel attacks on GPUs under Prof. Huiyang Zhou

Publications

Conferences

Z. Lin, **U. Mathur**, and H. Zhou, "Scatter-and-Gather Revisited: High-Performance Side-Channel-Resistant AES on GPUs", The 12th workshop on General-Purpose Computation on Graphics Processing Units (GPGPU-2019), 2019

PROJECTS

Design of a Side Channel Resistant Implementation of AES on GPUs — *Oct, 2018 - Dec, 2018*

- Proposed and implemented a high throughput masking based design of AES to mitigate timing based side channel attacks
- Studied performance of variants like S-Box, T-Table, Bitsliced, Rivain-Prouff, H-Table, and the proposed for different RNG configs

Operating Systems Design - XINU OS — *Sept, 2018 - Dec, 2018*

- Implemented virtual memory abstraction (including virtual stack space) on x86 using 4KB pages
- Implemented (1) multi-level feedback queue for process scheduling; (2) spin-lock, guard-lock, try-lock, and priority inheritence

Design and Side Channel Analysis of Quantum Secure Module — *Oct, 2018 - Oct, 2018*

- Designed and implemented an FPGA synthesizable module for Binary Learning with Errors (LWE), a Quantum Secure Module
- Performed power based side channel analysis on the designed module to extract secret information

Load Latency Hiding using Load Slice Buffer (LSB) and Load Value Prediction — *Mar, 2018 - May, 2018*

- Proposed and implemented a micro-arch for continual flow of instructions during retirement stall on L2 miss at head of ROB
- Implemented LSB in 721sim (cycle-accurate RISC-V superscalar simulator) to maintain fake-retired load dependent instructions
- Implemented re-insertion of the instructions in slice to issue queue on load value misprediction
- Implemented hierarchical store queue with membership test buffer (MTB) to prevent it from becoming a cycle time bottleneck

Multipath Execution for Divergent Control Flow in GPUs — *Feb, 2018 - May, 2018*

- Replaced SIMT stack with split table and reconvergence table in GPGPU-sim to allow interleaved execution of divergent paths
- Modified scoreboard logic to handle dependencies from diverged paths correctly

OoO Simulator — *Nov, 2017 - Dec, 2017*

- Developed a simulator for an out-of-order superscalar processor based on Tomasulo's algorithm that fetches, dispatches, and issues N instructions per cycle with integrated two level caches. Perfect branch prediction was assumed

Branch Predictor and Cache Simulator — *Sept, 2017 - Oct, 2017*

- Developed a generic cache simulator for WTWNA, WTWA and WBWA policies which could be used to instantiate any level of memory hierarchy with the option to augment victim cache. Replacement policies like LRU, LFU and LRFU were also incorporated
- Worked on a cache simulator for MESI, MOESI and MSI cache coherence protocols
- Developed a simulator for branch predictor with different configurations like GShare, BiModal, Hybrid with an option to add BTB